

1 **In the Claims**

2 Claims 1, 11 and 21 are currently amended.

3 Claims 1-26 remain in the application for consideration and are listed as
4 follows:

5
6 1. (Currently Amended) A method for use in a computer capable of
7 supporting multiple authentication mechanisms, the method comprising:
8 generating at least one indicator that identifies a user, and is associated with
9 and identifying identifies at least one authentication mechanism that has been used
10 to authenticate a the user; and
11 controlling the user's access to at least one resource based on the indicator.

12
13 2. (Original) The method as recited in Claim 1, wherein generating the
14 indicator further includes receiving inputs, providing the inputs to the
15 authentication mechanism, and causing the authentication mechanism to generate
16 at least one security identifier (SID) that identifies the authentication mechanism.

17
18 3. (Original) The method as recited in Claim 1, wherein generating the
19 indicator further includes identifying within the indicator at least one characteristic
20 associated with the authentication mechanism.

21
22 4. (Original) The method as recited in Claim 3, wherein the at least one
23 characteristic associated with the authentication mechanism includes a measure of
24 strength of the authentication mechanism.
25

1 5. (Original) The method as recited in Claim 4, wherein the measure of
2 strength of the authentication mechanism identifies a length of an encryption key
3 employed by the authentication mechanism.
4

5 6. (Original) The method as recited in Claim 1, wherein controlling
6 access to the resource based on the indicator further includes comparing the
7 indicator to at least one access control list having at least one access control entry
8 therein.
9

10 7. (Original) The method as recited in Claim 6, wherein if the access
11 control entry operatively specifies that the at least one authentication mechanism
12 is permitted to access the resource, then access to the at least one resource is
13 allowed to proceed.
14

15 8. (Original) The method as recited in Claim 6, wherein if the access
16 control entry operatively specifies that the at least one authentication mechanism
17 is not permitted to access the resource, then access to the at least one resource is
18 not allowed to proceed.
19

20 9. (Original) The method as recited in Claim 6, wherein if the access
21 control entry does not operatively specify that the at least one authentication
22 mechanism is permitted to access the resource, then access to the at least one
23 resource is not allowed to proceed.
24
25

1 10. (Original) The method as recited in Claim 1, wherein the indicator
2 includes a security token.

3
4 11. (Currently Amended) A computer-readable medium for use in a
5 device capable of supporting multiple authentication mechanisms, the computer-
6 readable medium having computer-executable instructions for performing acts
7 comprising:

8 producing at least one indicator that identifies a user, and uniquely
9 identifies at least one authentication mechanism supported by the device that has
10 been used to authenticate a the user; and

11 causing the device to selectively control the user's access to at least one
12 resource operatively coupled to the device based at least in part on the indicator.

13
14 12. (Original) The computer-readable medium as recited in Claim 11,
15 wherein producing the indicator further includes receiving inputs, providing the
16 inputs to the authentication mechanism, and causing the authentication mechanism
17 to generate at least one security identifier (SID) that identifies the authentication
18 mechanism, in response thereto.

19
20 13. (Original) The computer-readable medium as recited in Claim 11,
21 wherein producing the indicator further includes identifying within the indicator at
22 least one characteristic of the authentication mechanism.

1 14. (Original) The computer-readable medium as recited in Claim 13,
2 wherein the at least one characteristic of the authentication mechanism includes a
3 strength characteristic of the authentication mechanism.

4
5 15. (Original) The computer-readable medium as recited in Claim 14,
6 wherein the strength characteristic identifies a length of an encryption key
7 employed by the authentication mechanism.

8
9 16. (Original) The computer-readable medium as recited in Claim 11,
10 wherein causing the device to selectively control access to the at least one resource
11 based on the indicator further includes causing the device to compare the indicator
12 to control data .

13
14 17. (Original) The computer-readable medium as recited in Claim 16,
15 wherein if the control data specifies that the authentication mechanism is
16 permitted to access the resource, to which subsequent access to the resource is
17 allowed.

18
19 18. (Original) The computer-readable medium as recited in Claim 16,
20 wherein if the control data operatively specifies that the authentication mechanism
21 is not permitted to access the resource, to which subsequent access to the resource
22 is prohibited.

23
24 19. (Original) The computer-readable medium as recited in Claim 16,
25 wherein if the control data does not operatively specify that the authentication

1 mechanism is permitted to access the resource, to which subsequent access to the
2 resource is prohibited.

3
4 20. (Original) The computer-readable medium as recited in Claim 10,
5 wherein the indicator includes a security token.

6
7 21. (Currently Amended) An apparatus comprising:
8 at least one authentication mechanism configured to generate at least one
9 indicator that identifies a user, and identifies the authentication mechanism that
10 has been used to authenticate a the user;

11 an access control list;
12 at least one access controlled resource; and
13 logic operatively configured to compare the indicator with the access
14 control list and selectively control the user's access to the resource based on the
15 indicator .

16
17 22. (Original) The apparatus as recited in Claim 21, wherein the
18 authentication mechanism is further configured to receive user inputs and generate
19 at least one security identifier (SID) that identifies the authentication mechanism
20 based on the user inputs.

21
22 23. (Original) The apparatus as recited in Claim 21, wherein the
23 indicator further includes at least one identifying characteristic associated with the
24 authentication mechanism.

1 24. (Original) The apparatus as recited in Claim 23, wherein the at least
2 one identifying characteristic associated with the authentication mechanism
3 indicates a measure of strength of the authentication mechanism
4

5 25. (Original) The apparatus as recited in Claim 24, wherein the measure
6 of strength of the authentication mechanism identifies a length of an encryption
7 key employed by the authentication mechanism.
8

9 26. (Original) The apparatus as recited in Claim 23, wherein the
10 indicator includes a security token.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25